Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 2113 – 2117

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

Information Hiding for AES Core Based on Randomness

Hongying Liu[a,*] ,Ying zhou[b*], Yibo Fan[c*],Yukiyasu Tsunoo[d] ,Satoshi Goto[a]

[a]*Graduate School of Information, Production and Systems, Waseda University, Kitakyushu-shi, 8080135, Japan.*
[b] *Technology Center, ROHM Co.Ltd., Yokohama, 2228575, Japan*
[c]*State-key Lab of ASIC & System, Fudan University, Shanghai, 201203, China.*
[d]*Information and Media Processing Laboratories, NEC Corp., Kawasaki, 2118666, Japan*

Abstract

Advanced Encryption Standard (AES) is widely used symmetric cryptographic algorithm due to its ease in implementation on hardware and software. A number of works have been carried out on the reduction of power consumption of AES cores. Furthermore, the security of its implementation against side channel attacks also draws extensive attention. Various countermeasures that protect it from attack have been proposed. However not all of them is sufficient for high throughput applications. In this paper, we design and implement a differential power analysis (DPA) resistant AES core on Side-channel Attack Standard Evaluation Board. It is not only compact but also secure. The throughput is 2.56Gbps at 200MHz. By adding a set of registers and a random generator, the data-dependent encryption is hidden from observation. The experiments of DPA attack substantiate its effectiveness.

Selection and/or peer-review under responsibility of [CEIS 2011]

Keywords: Information hiding; AES; DPA attack; countermeasure; implementation.

* Corresponding author. Tel.: +86 18710758059

E-mail: liuhongying @fuji.waseda.jp, Ying.Zhou@dsn.rohm.co.jp, fanyibo@fudan.edu.cn

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2011.08.395

1. Introduction

Low power, high throughput and compactness have always been topic of interest for hardware design and implementation. As the security in digital devices attracts much attention, AES[1] is one of the most popular symmetrical encryption algorithms, which has been designed and implemented. A number of researches have been carried out on the reduction of power consumption of AES circuits [2]. Many circuit architectures have been proposed and their performances have been evaluated by using ASIC libraries [3]. However the security of cipher not only depends on its mathematical properties but also its implementations. DPA [4], which is based on exploiting the power consumption of cryptographic devices to reveal keys, has become a serious threat to the security.

Therefore, countermeasures that protect cryptographic devices from attack have been proposed. They mainly fall into two categories [5]: masking and hiding. Masking is a method that masks all the intermediate values of circuit by random number. A detailed design method of AES core with masking has been proposed in [6-8]. Hiding conceals the power consumption by inserting dummy operations, shuffling operations or adding power supply filter. In [9], it demonstrated an AES core with a switched-capacitor power filter. But it needs additional custom design for its power filter. Since the hiding method leaves intermediate values unchanged, it might causes potential risk in future. And there are flaws for masking in defending DPA attack, which has been proved [10].

Based on the above consideration, we devoted to the hiding countermeasure. Meanwhile, in order to achieve a high security level and take into account the implementation cost, we design and implement a DPA resistant AES core, which is not only compact in structure but also has high throughput. A set of registers and a random generator are added to protect AES from attacks.

The rest of the paper is organized as follows. Some related background is introduced in Section 2. Our design is described in Section 3. The implementation and results are shown in Section 4. The DPA resistant analysis is presented in Section 5. Conclusions are provided in Section 6.

2. Background

AES operates on a 4×4 array of bytes termed State. For encryption, it implements a round function 10, 12, 14 times (depends on the key length). The encryption data flow of AES algorithm is shown in Fig.1. Four transformations including SubBytes, ShiftRows, MixColumns and AddRoundKey are included in this encryption process. A separate Key Expansion unit is used to generate keys for each round of AES algorithm.

1) ShiftRows: In this operation, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes.

2) AddRoundKey: It is a 128-bit XOR operation performed to State and Key.

3) MixColumns: It is a 32-bit operation which operates on the columns of the State using a linear transformation.

4) SubBytes: It is an 8-bit operation, and it is a non-linear byte substitution that operates on each byte of the State using a substitution table.

3. Proposed information hiding method

DPA attack works because the power consumption of cryptographic device depends on intermediate values of the executed cryptographic algorithm. We design an information hiding method to make the power consumption of a cryptographic device independent of the intermediate values. Power consumed when the data in registers change from intermediate value to ciphertext/plaintext. Therefore we add a set

of data register to save intermediate value and ciphertext/plaintext separately. And these two sets of data register are in different position, shown in Fig.2. A random number generator is used to randomly choose which set to save the intermediate value, and make sure the ciphertext/plaintext are saved in the other set.

To determine the position of the two sets of registers, a nonlinear operation is requested when DPA attack choose the intermediate. And the only nonlinear operation in AES is SubBytes. If the two sets of register are in the same side of SubBytes the attacker can choose the first round or the last round of AES to analysis. So the two sets of register should be put in the two different sides of SubBytes. Fig.2 shows an example implemented in the SASEBO FPGA board.

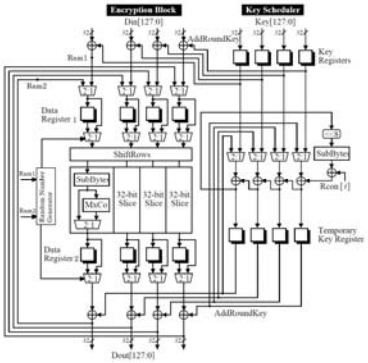


Fig. 2. Information hiding by registers

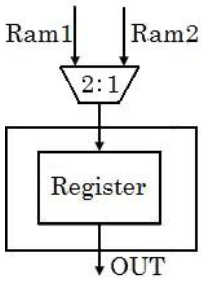


Fig. 3. Random Number Generator

The next consideration is that how to design a random number generator. We have only two choices about where is the data saved in each clock. So we need to generate a binary number to choose the upper set or down set of register. The random number generator in our method uses one bit register.

In the first round, we pick a binary number which is generated after exclusive OR of plaintext and the original key in the first round. In the other rounds, we pick one binary number of the former round's result. The random number generator is shown in Fig.3.

In each round of AES, we choose a set of register, thus attackers can't know the details of each round of AES. Take the last round attack for example; there are a lot of possibilities to overwrite the registers. By different situations, there are different ways to attack. But the attacker didn't know which way they can use in each time of AES encryption. So attackers can't attack AES successfully.

4. Physical implementation and comparison

Table 1. Results and comparisons.

	ESSCIR[6]	ASICON[7]	WiCOM[8]	Unprotected	Proposed
Technology	0.25μm	0.25μm	0.18μm	0.13μm	0.13μm
Gate Count	42408	48000	49000	24587	27046
Max Throughput	1.15Gbps	380Mbps	900Mbps	2.56Gbps	2.56Gbps
DPA resistant	Yes	Yes	Yes	No	Yes
Countermeasure	Mask	Mask	Mask	/	Hide

AES with proposed countermeasure is implemented in Verilog HDL, simulated with ModelSim and synthesized using Synopsys Design Compiler in TSMC 0.13 μm CMOS technology. The result is listed in Table1 and compared with other works. We achieve the maximal throughput 2.56 Gbps with 27046 gates count.

Compared with unprotected AES implementation, we can conclude that the proposed AES core with countermeasure increases 2.45k gates count but do not influent the throughput at all. It is worthy while to

add a little cost to achieve a strong defending capability. Compared with three other works, we can obviously find out that our work is a low cost and high throughput structure. So our proposal is a high speed and portable way to get a high security AES implementation.

5. Analysis of DPA resistance

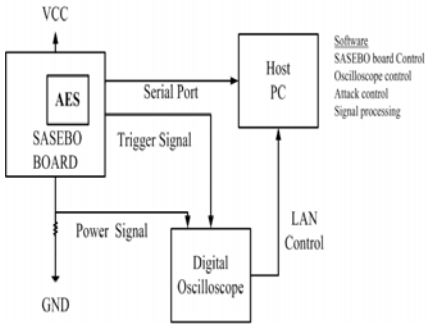


Fig.4. Implementation environment

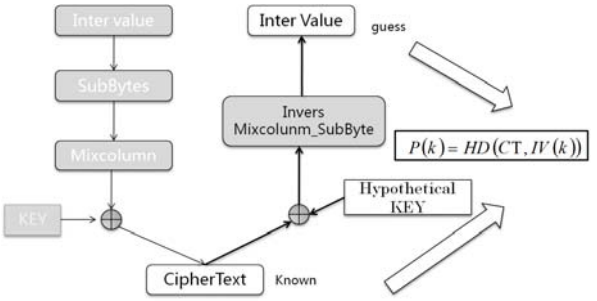
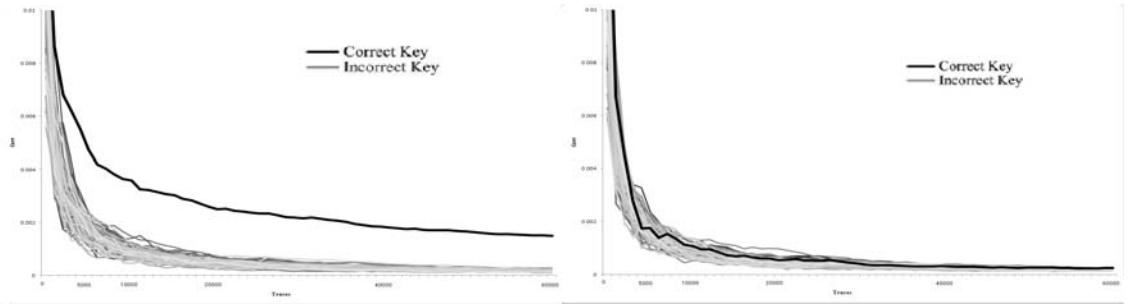


Fig.5. The flow of DPA attack on unprotected AES

We implement this AES structure which does not switch the register bit by bit on Side-channel Attack Standard Evaluation Board (SASEBO), which is provided by AIST [12].

The sketch of experimental environment is shown in Fig.4. The board is connected to the independent power supply. While the encryption is running, we use digital oscilloscope to retrieve the power traces. We record the power traces data when there is a trigger signal. After record the data, we transmit the data back to PC.



(a) (b)

Fig.6. The result of DPA attack test on AES implementation.(a)Result of unprotected AES.(b)Result of proposed AES.

Two types of data are transferred. The cipher text encrypted by the SASEBO device is transmitted to PC through RS232 serial port communication. On the other hand, the digitized power trace waveform data will be transmitted back through LAN. The power analysis attack is totally based on the power consumption data and the cipher text.

For attacking AES, a resistance is inserted in the GND or VDD. When the AES working, we can get the current through the resistance, so we can trace the power. The flow for attack is shown in Fig.5.

The result of attacking the unprotected AES is showed in Fig.6 (a), the black line is the right key, and it obviously outstands from other 255 candidates. The DPA attack result against proposed architecture is shown in Fig.6(b). It indicates that the right key can't be guessed out by adding our proposed countermeasure by more than double trace number. So we can also prove that if we randomly choose the

upper or down register bit by bit. Each bit of the data saved in different set of register. So in each block we can achieve a very high security as $\mathbf{2^8}$ times than unprotected AES.

6. Conclusions

In this paper, we design and implement a low cost AES core with countermeasure. By adding a set of register and a random number generator, the security is improved. The experiments on Side-channel Attack Standard Evaluation Board have proved its effectiveness. Because of its cost-efficiency, our design is suitable for low cost and high secure systems such as smart card, embedded systems, etc. In the future, other countermeasures, which can resist higher order attacks will be studied and implemented.

Acknowledgements

This work was supported by Waseda University “Global COE program” and CREST of JST in Japan.

References

[1] National Institute of Standards and Technology (NIST) of U.S. Department of Commerce: FIPS 197: Advanced Encryption Standard”, Nov. 2001.

[2] S.Morioka and A.Satoh, “An Optimized S-Box Circuit Architecture for Low Power AES Design”, Proc.of CHES 2002, LNCS2523, pp.172-186,2002.

[3] Y.Zeng, X.Zou, and Z.Liu, et.al, “A low-power Rijndael S-Box based on pass transmission gate and composite field arithmetic”, Journal of Zhejiang University SCIENCE A, Vol.8(10),pp.1553-1559, 2007.

[4] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, Advances in Cryptology: Proceedings of CRYPTO’99, number 1666 in Lecture Notes in Computer Science, pages 388–397, Santa Barbara, CA, USA, August 15-19 1999. Springer-Verlag.

[5] S. Mangard, E. Oswald, and T. Popp, “Power Analysis Attacks: Revealing the secrets of smart card,” published by Springer, 2007.

[6] N. Pramstaller, F.K. Gurkaynak, S.Haene, et al, "Towards an AES crypto-chip resistant to differential power analysis", Proceeding of the 30th Solid-State Circuits Conference, ESSCIRC 2004, pp. 307- 310, Sept. 21-23, 2004.

[7] J. Zhao, J. Han, X.Y. Zeng, J. Chen, "VLSI implementation of an AES algorithm resistant to Differential Power Analysis attack", 7th International Conference on ASIC (ASICON 2007), pp.838-841, Oct. 2007.

[8] X. Zheng, Y. Zhang，"Design and Implementation of a DPA Resistant AES Coprocessor", proc. of 4th International conference on Wireless Communications, networking and Mobile computing(WiCOM08), 2008.

[9] C.Tokunaga, D.Blaauw, "Secure AES Engine with a local switched-capacitor current equalizer",Proceedings of 2009 IEEE international Solid-State Circuits Conference,pp.64-66,2009.

[10] M. Saeki, D. Suzuki, and T.ichikawa, “Leakage analysis of DPA Countermeasures at the Logic Level ”,IEICE Transactions on Fundamentals, Vol.E 90-A, No.1,pp.169-178,2007.

[11] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model”, Proc. of CHES 2004, LNCS 3156, pp. 16-29, 2004.

[12] SASEBO project in Research Center for Information Security (RCIS). www.rcis.aist.go.jp/special/SASEBO/